roved for use through 10/31/99. OMB 0651-0031 ark Office: U.S. DEPARTMENT OF GOLMERCE

				Tutont and True	ciliar Office. C.b. Derra	CTIME OF TO PRODUCE
	()		·	C	OMPLETE IF KNO	WN D. C.
Substitute for	form 1449A/PTO			Application Number	09/534,836	The CC V
	INFORMATION	I DISCLOSUI	RECIPE	Filing Date	March 24, 2000	Chron 8
	STATEMENT B	Y APPLICAT	<b>(1</b> )	Nirst Named Inventor	C. Andrew Neff	1000 COO
		(	DEC 0 5 2000	LGroup Art Unit	.2766	SIME
	(use as many she	ets as necessary	to the	xaminer Name		270
Sheet	1	of	Terra 2 COMPET	Attorney Docket No.	32462-8004US	9
			THRU			

			U.S. PATEN	T DOCUMENTS	5				
*EXAMINER INITIALS	Cite No.	U.S. Patent Document  NUMBER Kind Code (if known)	Name of Patent of Cited I	ee or Applicant Document	Date of Publication of Cited  Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear			
F.b.	AA	5,495,532	Kilian et al.		2/27/96				
1	AB	5,521,980	Brands		5/28/96				
	AC	5,682,430	Kilian et al.		10/28/97	-			
E.D.	AD	5,878,399	Peralto		3/2/99				
<u> </u>	AE	, ,							
	AF								
	AG					M1			
	AH								
	AI								
<del></del>	AJ								
			FOREIGN PAT	ENT DOCUME	NTS				
*EXAMINER INITIALS <sup>*</sup>	Cite No.	Foreign Patent Document Kind Office Number (if kn	Name of			Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Т		
-	AK	Office Number (II Kil	j.						
	AL								
	AM				-				
<del>,</del>	AN								
	AO								
		OTHER PRIO	P ART-NON PA	FENT LITERAT	URE DOCUMENT	'S			
*EXAMINER INITIALS*	Cite No.	Include name of the au	thor (in CAPITAL LETTI	ERS), title of the article (w	hen appropriate), title of the	item (book, magazine,	Т		
FB.	AP	Benaloh, J., "Secret S	journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.  Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987						
ı	AQ	Benaloh, J., et al., "Di				acy of Voters", ACM			
F.B.	AR	Symposium on Principl Cramer, R., et al., "Pr CRYPTO 1994, Lecture	oofs of Partial Kno	wledge and Simplif	fied Design of Witnes		-		

EXAMINER //				DATE CONSIDERED						
1 Fr	·····	Sou		6/11	/03					
* EXAMINER:		nce considered, whether not considered. Include				Draw lin	e through	citation	if no	ot in

					Patent and Trac	demark Office: U.S. DEPARTM	
					C	COMPLETE IF KNOWN	, CA
Substitute f	for form 1449	9A/PTO		(10)	Application Number	09/534,836	E 1/2
	INFO	RMATION	DISCLOSU	BEOIPE	Filing Date	March 24, 2006/2	0,
			Y APPLICA	NT	irst Named Inventor	C. Andrew Neff	2 300
			(	DEC 0 5 2000	யிroup Art Unit	2766	Con
	(use	as many she	ets as necessary		Examiner Name		10 J
Sheet		2	of	To Transment	Attorney Docket No.	32462-8004US	9
		OTHE	R PRIOR AR	RT-NON PATE	NT LITERATURE	DOCUMENTS	
EXAMINER	Cite No.					propriate), title of the item (book	

		OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS	
*EXAMINER INITIALS*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.	Т
F.p.	AS	Cramer, R., et al., "Multi-Authority, Secret-Ballot Elections with Linear Work", Advances in Cryptology – EUROCRYPT 1996, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996	
1	AT	Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in Cryptology – EUROCRYPT 1997, Lecture Notes in Computer Science, Springer-Verlag, 1997.	
	AU	Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182	
	AV	Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981	
	AW	Diffie, W., et al., "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654, 1976	
	AX	ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4):469-472, 1985	
	AY	Fujioka, A., et al., "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology – AUSCRYPT 1992, Lecture Notes in Computer Science, pp. 244-251, Springer-Verlag, 1992	
	AZ	Fiat, A., et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 186-194, Springer-Verlag, New York, 1987	
	BA	Gennaro, R., "Achieving independence efficiently and securely", Proceedings 14 <sup>th</sup> ACM Symposium on Principles of Distributed Computing (PODC 1995), New York 1995	
	BB	Iversen, K., "A Cryptographic Scheme for Computerized General Elections", CRYPTO 1991, pp. 405-419	
	ВС	Odlyzko, A. M., "Discrete logarithms in finite fields and their cryptographic significance", Advances in Cryptology – EUROCRYPT 1984, Notes in Computer Science, Springer-Verlag, 1984	
	BD	Park, C., et al., "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science, pp. 248-259, Springer-Verlag, 1993	
	BE	Pedersen, T., "A Threshold Cryptosystem without a Trusted Party", Advances in Cryptology – EUROCRYPT 1991, Lecture Notes in Computer Science, pp. 522-526, Springer-Verlag, 1991	
	BF	Sako, K., et al., "Secure Voting Using Partially Compatible Homomorphisms", Advances in Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, Springer-Verlag, 1994	
	BG	Sako, K., et al, "Receipt-Free Mix-Type Voting Scheme – A practical solution to the implementation of a voting booth –, EUROCRYPT 1995, pp. 393-403	
	ВН	Schnorr, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 4(3):161-174, 1991	,
	BI	Schoenmakers, B., "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", Advances in Cryptology – CRYPTO 1999, Lecture Notes in Computer Science, pp. 1-17, Springer-Verlag 1999	
FB.	BJ	Shamir, A., "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979	

EXAMINER	Λ		DATE CONSI	IDERED		
	u	bort		1		
	~~~~		6/	11/03		
* EVANINDO.	7 2 2 2			W MED COO	Dunne line theresal	

\* EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Clients\VoteHere, Inc.(32462)\8004 - Authentication\US\SB08.doc

OIPE VOS

					w 7 1	<b>उठका</b> हैं।	Patent	and Trad	Approved for use in emark Office: U.S. I	rough 10/31/99. OMB 0651-0 DEPARTMENT OF COMMEI	RCE
				M	Ki c	5			OMPLETE IF R	KNOWN	
Substitute f	for form	1449A/PTC	<b>)</b>		95 <b>%</b>	OOEMAR	Application Num	her	09/534,836	REOF	
o dostituto i	INF		ATION D	SCL	OSU	RE	Confirmation Nu		2620	- CE	VF
	ST	ATEM	ENT BY	APPL	.ICA	NT	Filing Date		March 24, 200	RECEIVE MAY 2 3 2	
			any sheets				First Named Inve	entor	C. Andrew No	eff "' Z J	20ก
	,		•			•	Group Art Unit		2766	Technology Cente	
							Examiner Name			Centi	er 2
Sheet		1		of		1	Attorney Docket N	lo.	32462-8004U	S	
						U.S. PATENT	DOCUMENT	S			
*EXAMINER	Cite		. Patent Docume			Name of Patentee or		Date of	f Publication of Cited	Pages, Columns, Lines, Where Relevant Passages or	
INITIALS	No.	NUMBE		d Code known)		of Cited Docu	ment		Document	Relevant Figures Appear	
1.0	AA	5,717,	759		Mic	ali		2/10/	98		
F.B.	AB	5,864,	667		Barl	kan		1/26/	99		
	AC										
	AD										
	AE	·	<del></del>					-			
	AF										
	AG										
	AH					•					
	AI										
	AJ										
		ı		<u> </u>	FO	REIGN PATE	NT DOCUME	NTS			
*EXAMINER	Cite	I	Foreign Patent D	ocument		Name of Pa	tentee or Applicant	I	Date of Publication of	Pages, Columns, Lines, Where Relevant Passages or Relevant	T
INITIALS*	No.	Office	Number	Kind (if kn		of Cite	ed Document	4	Cited Document	Figures Appear	1
F.15.	AK	wo	98/14921			Certco, LLC		4	/9/98		
	AL										
	AM										
	AN										
	AO										
	· · · · · · · · · · · · · · · · · · ·	l	OTHER I	PRIO	RAF	RT-NON PATE	NT LITERAT	URE	DOCUMENT	S	<del></del>
*EXAMINER INITIALS*	Cite No.									item (book, magazine, puntry where published.	Т
Fis	AP	Borrel	l, Joan et a	l., "A	n imp		e voting scheme			ity, Elsevier Science,	
	AQ					sus: A Security ternational Confe				n for the Internet", pp. 561-570	
F.B	AR					Secure E-Voting EE 1998, pp. 293-		", Proc	eedings, Annua	l Computer Security	
EXAMINE	ER		~ b.	orh	_		DATE CONS		ED 9/04		
* EXAMIN	ER:	Initial if	reference co	nsidered	i, whet	her or not criteria				line through citation if no	t in

conformance and not considered. Include copy of this form with next communication to applicant(s).

gh 10/31/99. OMB 0651-0031 ARTMENT OF COMMERCE

		4	ved	for	use t	hroug
atent	and	Trader	Offi	ice:	U.S.	DEP

#9	
#9	

JUN 2 5 2001 r form 1449A/PTO
INFORMATION ELSCHOOTER Substitute for form 1449A/PTO STATEMENT BY APPLICANT

(use as many sheets as necessary)

**COMPLETE IF KNOWN** 09/534,836 Application Number 2620 Confirmation Number March 24, 2000 **Filing Date** C. Andrew Neff First Named Inventor 2766 Group Art Unit

						Examiner Name				
Sheet		.1	of		1	Attorney Docket N	No.	32462-8004US		
			<u> </u>	Ţ	J.S. PATENT	DOCUMENT	S			
*EXAMINER INITIALS <sup>*</sup>	Cite No.	U.S. Patent I	Nocument Kind Code (if known)		Name of Patentee or of Cited Docum		Date of Publication of Cited  Document		Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	
r. b.	AA	5,278,753	(II KIIOMI)	Graf	t, III		1/11/94			
E.D.	AB	5,400,248		Chis	holm		3/21/	95	- Pr	
17.	AC								MECEIVED	
	AD						<u> </u>		RECEIVED	
	AE								hnology Center 2600	
	AF								3 Center 2600	
	AG									
	AH									
	AI						<u> </u>			
	AJ									
				FO	REIGN PATE	NT DOCUMI	ENTS			_
*EXAMINER INITIALS*	Cite No.			Code		atentee or Applicant ted Document		Date of Publication of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	
	AK	Office	unoci (ii ii					4/9/98		1
	AL					•				$\perp$
	AM									$\downarrow$
	AN									4
	AO									
		OTH	IER PRIC	R Al	RT-NON PATI	ENT LITERA	TURE	E DOCUMENT	rs	_
*EXAMINER	Cite			.1 .	CARTAL LETTER	C) title of the article	(when ar	oppopriate), title of the	item (book, magazine, ountry where published.	
INITIALS	No.	Journal,	serial, sympos	Secure	Flectronic Voti	ng Protocol with	ı IC Ca	rds", Elsevier Sc	cience Inc., New York,	
F.B.	AP	J. Systems	Software 19	97, 39	9:93-101					
<u> </u>	+									
	AQ	!						<u> </u>		+
	AR									
EXAMIN		<del>)                                    </del>				DATE CO		/ /		
,	7	ć	ba	<b></b>	•			11/03		
* EXAMI	MER:	Initial if refer	ence consider	ed, who	ether or not criteria	is in conformance	e with		line through citation if	not

conformance and not considered. Include copy of this form with next communication to applicant(s).

## COMP E IF KNOWN 09/534,836 Application Number INFORMATION DISCLOSURE STATEMENT BY APPLICANT Confirmation Number 2620 iling Date March 24, 2000 Form PTO-1449 (Modified) rst Named Inventor C. Andrew Neff (Use several sheets if necessary) 2131 Group Art Unit Examiner Name Gail O. Hayes 1 of Attorney Docket No. 324628004US

				Ĺ	I.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	•	U.S. Patent or Application  Kind Code  NUMBER (if known)		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	5,		
	_									
		_					RECEIVED			
							CEP 2 6 2002			
					,	Te	SEP 2 6 2002 chnology Center 2100			
								$\dashv$		
			<u> </u>					$\dashv$		
				FOE	REIGN PATENT DOCUMENTS					
Examiner	Cite	Fore	eign Patent or Appli		Name of Patentee or Applicant	Date of Publication or Filing Date of Cited	Pages, Columns, Lines, Where Relevant			
Initial	No.	Office	NUMBER	(if known)	of Cited Document	Document	Figures Appear	T		
F.B		EP	0 697 776	A2	NEC Corporation	2/21/96		Ш		
F.B.		EP	0 743 620	A2	NEC Corporation	11/20/96				
					·		-			
					T-NON PATENT LITERATURE [					
Examiner Initials	Cite No.	<b>(</b> b	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.							
								+		
	l	l								

EXAMINER /	/ · /	DATE CONSIDER	ERED					
$\varphi$	Son	1 (	/11/03					
1 free		0/	1/1/03					
*EXAMMER:	Initial if reference considered, whether or not criteria is in confor	mance with MPEP 60	609! Draw line through citation if not in conformance and not					
	considered. Include copy of this form with next communication to application(s).							

Sheet



## INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Form PTO-1449 (Modified) (Use several sheets if necessary)

of

COMPLETE IF KNOWN				
Application Number	09/534,836			
Confirmation Number	2620			
Filing Date	March 24, 2000			
First Named Inventor	C. Andrew Neff	_		
Group Art Unit	2131			
Examiner Name	Gail O. Hayes			
Attorney Docket No.	324628004US			

**U.S. PATENT DOCUMENTS** Date of U.S. Patent or Application Publication or Filing Date Pages, Columns, Lines, Cite of Cited Kind Code Name of Patentee or Inventor Where Relevant Examiner NUMBER (if known) of Cited Document Document Initials No. Figures Appear 5,708,714 López et al. 1/13/98 .6. RECEIVED OCT 0 \$ 2002 Technology Center 2100 FOREIGN PATENT DOCUMENTS Date of Foreign Patent or Application Publication or Filing Date Pages, Columns, Lines, Examiner Cite Kind Code Name of Patentee or Applicant of Cited Where Relevant of Cited Document Document Т Initial No. Office NUMBER (if known) Figures Appear OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published. Examiner Cite Т Initials No.

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEF 609. Oraw line through citation if not in conformance and not							
considered. Include copy of this form with next communication to application(s).							
F							

	IPR						
/9	3					PLETE IF KNOWN	
	1 2 2002 TO	1			Application Number	09/534,836	
<b>\</b>	101	INFORMATION			Confirmation Number	2620	
STATEMENT BY APPLICANT				Filing Date	March 24, 2000		
Form PTO-1449 (Modified)  (Use several sheets if necessary)					First Named Inventor	C. Andrew Neff	
		(Use several she	se several sheets if necessary)		Group Art Unit	2131	
		<b></b>	<u>,</u>		Examiner Name	Gail O. Hayes	
	Sheet	1	of	1	Attorney Docket No.	324628004US	

Cita	U.S	S. Patent or	A 1: 4:			Data of		
U.S. Patent or Application  miner Cite Kind Code (if known)		de	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear			
	6,081,793			Challene	Challener et al.	6/27/00		
					· · · · · · · · · · · · · · · · · · ·	REC	EIVED	
						NOV .	3 2002	
		0				Technology	Center 2100	
				FO	REIGN PATENT DOCUMENTS			
Cite	Fore Office		Kind	Code	Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	Т
	PCT	WO92/	03805	A1	Tecnomen Oy	3/5/92		
	PCT	WO01/	22200	A2	VoteHere, Inc.	3/29/01		
Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.							
	Cranor, L. F., "Electronic Voting, Computerized polls may save money, protect privacy," Crossroads, The ACM's First Electronic Publication, May 6, 1999, 4 pages							
	Herschberg, M. A., "Secure Electronic Voting Over the World Wide Web," Massachusetts Institute of Technology, May 27, 1997, 81 pages							
	No.	Cite No. Office PCT PCT  Cite No. Cranc privace Herse	Cite No. Office NUMBER PCT WO92/ PCT WO01/  OTH Cite No. Cranor, L. F., privacy," Cros	Cite No. Office NUMBER (if keep PCT WO92/03805  PCT WO01/22200  OTHER PRIOR (book, magazine, journal privacy," Crossroads  Herschberg, M. A., "S	Cite No. Office NUMBER (if known) PCT WO92/03805 A1 PCT WO01/22200 A2  OTHER PRIOR AR Include name of the author (book, magazine, journal, serial, No.  Cranor, L. F., "Electronic privacy," Crossroads, The	Cite No. Office NUMBER (if known) of Cited Document  PCT WO92/03805 A1 Tecnomen Oy  PCT WO01/22200 A2 VoteHere, Inc.  OTHER PRIOR ART-NON PATENT LITERATURE I Include name of the author (in CAPITAL LETTERS), title of the article (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s) and/or country where published.  Cranor, L. F., "Electronic Voting, Computerized polls privacy," Crossroads, The ACM's First Electronic Published.  Herschberg, M. A., "Secure Electronic Voting Over the content of the privacy of	FOREIGN PATENT DOCUMENTS    Foreign Patent or Application	Cite No. Office NUMBER (if known) Name of Patentee or Applicant of Cited Document of Cited Document of Cited Document Sigures Appear Pages, Columns, Lines, Where Relevant Figures Appear PCT WO92/03805 A1 Tecnomen Oy 3/5/92  PCT WO01/22200 A2 VoteHere, Inc. 3/29/01  OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS  Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.  Cranor, L. F., "Electronic Voting, Computerized polls may save money, protect privacy," Crossroads, The ACM's First Electronic Publication, May 6, 1999, 4 pages  Herschberg, M. A., "Secure Electronic Voting Over the World Wide Web,"

EXAMINER Sour	DATE CONSIDERED 6/1/03							
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).								